PROTECTING YOURSELF WHILE USING THE INTERNET

PERSONAL INFORMATION - Think before you post anything online or share information in emails. What you post online, can be seen by anyone. Sharing personal information with others you do not know personally is one of your biggest risks online. Sharing sensitive information such as your address, phone number, family members' names, car information, passwords, work history, credit status, social security numbers, birth date, school names, passport information, driver's license numbers, insurance policy numbers, loan numbers, credit/ debit card numbers, PIN numbers, and bank account information is risky and should be avoided. Consider removing your name from websites that share your personal information obtained from public records (including your phone number, address, social media avatars, and pictures) with anyone on the internet.

PHOTOS - Photos taken from smartphones embed the GPS Coordinates in the photo, which will allow others to know the location of where the picture was taken and may be used to find you. Beware of this when posting photos to online social media sites. Remember that pictures posted online may be copied, altered, and shared with many people without your knowledge or consent, unless you use privacy settings to limit who has access to the pictures.

EMAILS, PHISHING, AND MALWARE - Beware when opening emails from unknown people or sources, especially when they are unsolicited. Clicking on links or downloading attachments can infect your computer with a virus or subject you to fraud, malware, or a scam. Some viruses harm your computer, while others have the ability to steal your personal information and ultimately your identity. Be skeptical when receiving emails that look as if they came from your bank or other financial institution particularly if they ask you to verify or enter personal or financial information. Beware of scams that use links in emails directing you to a website or providing you with a phone number to call. Some links in emails can be deceiving. Consider typing in your own link to the banks and companies or look up the phone number yourself. In general, beware of email scams and websites that try to trick you into sharing your personal information. A website that looks legitimate can be set up quickly. Remember legitimate customer service representatives will never ask you for personal information or passwords. Consider not responding to unsolicited emails, never click on links in these emails, and be cautious if you are asked to respond quickly. Consider purchasing or downloading a good antivirus suite with spyware protection.

UPDATES - Keep your computer's operating system, browsers, antivirus, and other software up to date with the latest or daily security patches. For additional information visit http://www.uscert.gov/cas/tips/

PASSWORDS - Choose strong passwords using 10 characters and combinations of upper case letters, lower case letters, symbols, and numbers. Do not include personal information. Consider changing your password at least every 90 days when information is sensitive. Never leave passwords near your computer or in plain sight. Use different passwords for various online activities because if one password is compromised, all will be compromised. Never share your password. If given a choice to set up a password "hint" on an account, do not choose something others can easily guess.

SOCIAL - Beware of meeting people in-person whom you meet on the internet or through emails. Not everyone is honest with their identity, age, gender, and intentions. If necessary, do your research using public records and consider seeking reputable references. If you decide to meet someone, never go alone, let others know where you are going, meet in a very public place, and have your cell phone readily available.

PROTECTING YOURSELF WHILE USING THE INTERNET

EDUCATING CHILDREN/TEENS - Talk to and educate your children about internet risks and dangers of internet predators. Tell them never to meet people they met online in-person and never talk to people they really don't know. Discuss the importance of not posting identifying information, sensitive information, pictures, and details of upcoming activities on the internet. Be sure they understand what someone portrays on the internet may not be true. Teach them what they post online anyone can see unless they carefully control the privacy settings. Spend time with your child on the internet, know their favorite online destinations, know their passwords, limit the time they spend online, and consider placing the computer in a public room in the house. Periodically review your child's computer and emails. Know who your kids are chatting with online. For more information visit http://www.projectsafechildhood.gov

PARENTAL CONTROLS - Parents should consider applying parental controls by their internet service provider and/ or blocking software on family computers and smartphones to limit the internet to safe websites. Contact your internet provider if you have questions. Be sure to research your options regarding parental controls on products.

WEBCAMS - Be careful when using webcams. They can be high-jacked and turned on remotely. This allows others to illegally view and listen to individuals without their knowledge. Consider turning them off or disconnecting them when not in use. Limit or do not allow your children to use webcams and talk to them about the risks.

WIRELESS - Beware when connecting your laptop or mobile device to unsecured networks. Computer hackers on the same network can intercept your internet use and in some cases access files on your computer. Consider password protecting your home wireless network and using a personal firewall program for additional protection. For additional information visit http://www.uscert.gov/cas/tips/

SHOPPING - Avoid purchasing goods and services from websites that do not have secure check-out using "HTTPS." Pay attention to the address line on the checkout page which asks you to enter your credit card information. If the page does not have an "S" following "HTTP" in the address line, consider shopping somewhere else. Be aware that some information transmitted on HTTP pages is done so using plain text which can be intercepted by computer hackers.

SELLING - Beware of selling and listing items in local ads or elsewhere online. Never meet someone alone. If necessary, consider meeting in a public place, like a post office or bank rather than a parking lot. Beware of posting photos taken from smartphones for online adds. You could be sharing your home address with a criminal.

PUBLIC COMPUTERS - Avoid typing sensitive information on public computers, such as those in a public library or an internet café. Spyware may be installed on these computers that record your every keystroke. Also, you never know who may be watching your activity. Never select the feature that automatically signs you on to email or check any box to "Remember my Password" or websites.